equipment.

18. The cryptographic communication system according to claim 17 wherein:

(1) said IC card further includes a receiver for receiving said challenge data generated by said authentication equipment and transmitted via said intermediary equipment, and a response data transmitter for transmitting said encrypted data representing response data, said IC card ID data, and said certificate of individual IC card key data to said authentication equipment via said intermediary equipment;

(2) said means for producing said secret key in said authentication equipment includes a storage unit for storing a validation key, a second decryption unit for producing an IC card ID and a secret key by decrypting said certificate of individual IC card key data received from said IC card, using said validation key; and

(3) said authentication equipment further includes a challenge data generator / storage unit for generating and storing said challenge data, and a second matching determination unit for determining if said response data decrypted by said first decryption unit matches with said challenge data stored in said challenge data generator / storage unit.

19. The cryptographic communication system according to claim 18 wherein:

(1) said IC card further includes a combiner for generating combined data by combining said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and transmitting said combined data to said authentication equipment; and

(2) said authentication equipment further includes a first divider for dividing said combined data received from said IC card into said IC card ID data, said certificate of individual IC card key data, and said encrypted data, and a second divider for dividing data decrypted by said second decryption unit into said IC card ID and said secret key.

20. The cryptographic communication system according to claim 19 wherein said authentication equipment further includes a first combiner for combining said challenge data stored in said challenge data generator / storage unit and said IC card ID data produced by said second divider, a third divider for producing said challenge data from data combined by said first combiner, a second combiner for combining said response data decrypted by said first decryption unit and said IC card ID data produced by said second divider, and a fourth divider for producing said response data from data combined by said second combiner.

21. An electronic toll collection ("ETC") authentication system including an IC card, roadside equipment, and central processing equipment, comprising:

(1) said IC card including an encryption means for receiving a challenge data generated by roadside equipment, as said IC card passes said roadside equipment, and for encrypting said challenge data using a secret key; an encrypted data storage means for storing data encrypted by said encryption means; a response data transmission means for transmitting IC card ID data and a certificate of individual IC card key, together with said encrypted data stored in said encrypted data storage means, as response data to said roadside equipment;

(2) said roadside equipment including a dividing means for dividing said transmitted response data ; a second decryption means for decrypting said

certificate of individual IC card key data divided by said dividing means, using a validation key; a first matching determination means for making a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said dividing means; a first decryption means for producing response data by decrypting an encrypted data provided by said dividing means; and a challenge data transmission means for transmitting said challenge data to said IC card; and

(3) said central processing equipment including challenge data storage means for storing said challenge data generated by said roadside equipment; and a second matching determination means for receiving said response data decrypted by said first decryption means, and executing a matching determination of said response data with said challenge data stored in said challenge data storage means,

said ETC authentication system providing authentication of said IC card ID by said roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment.

22. An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) encrypting challenge data using a secret key in an IC card, said challenge data being generated by roadside equipment and transmitted to said IC card when said IC card passes by said roadside equipment;

(2) storing said encrypted data;

(3) transmitting an IC card ID data and a certificate of individual IC

card key data, in addition to said stored encrypted data, as response data to said roadside equipment;

(4) dividing said response data received by said roadside equipment ;

(5) decrypting said certificate of individual IC card key data, provided by the dividing step, using a validation key;

(6) carrying out a matching determination of an IC card ID provided in the decrypting step with another IC card ID provided in the dividing step;

(7) providing a response data by decrypting said encrypted data provided in the dividing step; and

(8) carrying out in said central processing equipment a matching determination of said response data decrypted by said roadside equipment with said challenge data,

said ETC authentication method providing authentication of said IC card ID by said roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing a matching determination of said response data encrypted by said IC card and decrypted by said roadside equipment.

23. An electronic toll collection ("ETC") authentication system comprising:

(1) first roadside equipment including challenge data and time generator / storage means for generating and storing challenge data and time information, and transmitting said challenge data and time information to an IC card;

(2) said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data and said time information generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting received data using a secret key; a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as a response data to a second roadside equipment;

(3) said second roadside equipment including a first dividing means for dividing said response data ; a second decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of an IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for producing a response data by decrypting an encrypted data obtained from said first dividing means; and

(4) central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated by said first roadside equipment; a third dividing means for dividing said response data and said IC card ID decrypted by said second roadside equipment; and a second matching determination means for making a matching determination of said challenge data obtained by said second dividing means and said response data provided by said third dividing means,

said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC

card and decrypted by said second roadside equipment.

24. The ETC authentication system according to claim 23, wherein said second roadside equipment further comprises another decryption means for decrypting said encrypted data provided by said first dividing means, using a secret key reproduced by said second decryption means; and a validation means for providing time information, at which said IC card passed said first roadside equipment, from a decrypted result of said another decryption means, and for confirming if a difference between said time information and present time is within a predetermined time period.

25. An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) receiving a card ID from an IC card before said IC card passes first roadside equipment;

(2) encrypting challenge data and time information using a secret key, said challenge data and time information being generated by first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment;

(3) transmitting IC card ID data and a certificate of individual IC card key data, in addition to said encrypted data, as a response data to second roadside equipment;

(4) dividing said transmitted response data in said second roadside equipment;

(5) decrypting said certificate of individual IC card key data provided in the dividing step using a validation key;

(6) carrying out a matching determination of an IC card ID provided in the decryption step with another IC card ID provided in the dividing step;

(7) providing a response data by decrypting said encrypted data provided in the dividing step;

(8) carrying out in central processing equipment a matching determination of said challenge data provided from said first roadside equipment and said response data decrypted in said second roadside equipment,

said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

26. The ETC authentication method according to claim 25 further comprising the steps of:

(1) decrypting said encrypted data provided by the dividing step, using a secret key reproduced in said decryption step; and

(2) providing time information, at which said IC card passed said first roadside equipment, as a result of the decryption step, and confirming if a difference between said time information and present time is within a predetermined time.

27. An electronic toll collection ("ETC") authentication system comprising:

(1) a first roadside equipment including a challenge data generation means for generating a challenge data, and transmitting said challenge data to an

IC card;

(2) said IC card including an ID transmission means for transmitting an IC card ID before said IC card passes said first roadside equipment; an encryption means for receiving said challenge data generated by said first roadside equipment, as said IC card passes said first roadside equipment, and encrypting said challenge data using a secret key; and a response data transmission means for transmitting an IC card ID data and a certificate of individual IC card key data, together with said encrypted data as response data to second roadside equipment;

(3) said second roadside equipment including a first dividing means for dividing said response data; a decryption means for decrypting said certificate of individual IC card key data divided by said first dividing means, using a validation key; a first matching determination means for providing a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by said first dividing means; and a first decryption means for decrypting an encrypted data provided by said first dividing means to obtain response data;

(4) central processing equipment including a second dividing means for dividing said challenge data and said IC card ID generated in said first roadside equipment; a third dividing means for dividing said response data decrypted in said second roadside equipment and said IC card ID; and a second matching determination means for providing a matching determination of said challenge data obtained in said second dividing means and said response data obtained in said third dividing means,

said ETC authentication system providing authentication of said IC card ID by said second roadside equipment by authenticating signature

information received with said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.

28. An electronic toll collection ("ETC") authentication method comprising the steps of:

(1) receiving a card ID from an IC card before said IC card passes by first roadside equipment;

(2) encrypting a challenge data using a secret key, said challenge data being generated by said first roadside equipment and transmitted to said IC card when said IC card passes said first roadside equipment;

(3) transmitting each individual data of said IC card ID and a certificate of individual IC card key, in addition to said challenge data encrypted in the encryption step, as response data to second roadside equipment;

(4) dividing said response data transmitted in the transmission stepby said second roadside equipment;

(5) decrypting said certificate of individual IC card key data divided in the dividing step, using a validation key;

(6) carrying out a matching determination of said IC card ID produced as a result of decryption with another IC card ID provided by the dividing step;

(7) producing a response data by decrypting said encrypted data provided by the dividing step; and

(8) executing in central processing equipment a matching determination of said challenge data provided by said first roadside equipment and

said response data decrypted by said second roadside equipment,

said ETC authentication method providing authentication of said IC card ID by said second roadside equipment by authenticating signature information received said IC card ID, and said central processing equipment providing the matching determination of said response data encrypted by said IC card and decrypted by said second roadside equipment.